ABSTRACT

In a serverless distributed file system, the writer of a file can provide file authentication information to a verifying machine without having to compute a new digital signature every time a written file is closed. Periodically, the writer compiles a list of the hash values of all files that have been written over a recent interval, computes a hash of the list, and signs the hash. This signed list of hash values is known as a manifest, akin to a shipping manifest that enumerates the items in a shipment. The advantage of using a signed manifest is that the writer need only perform a single signature computation in order to authenticate the writes to multiple files, rather than having to compute a separate signature for each file, as it would if a signature were embedded in each file.